A Security Management Framework for Routing Protocols: RPsec

draft-atwood-rtgwg-rpsec

William Atwood
Nitin Prajapati

Routing Protocols

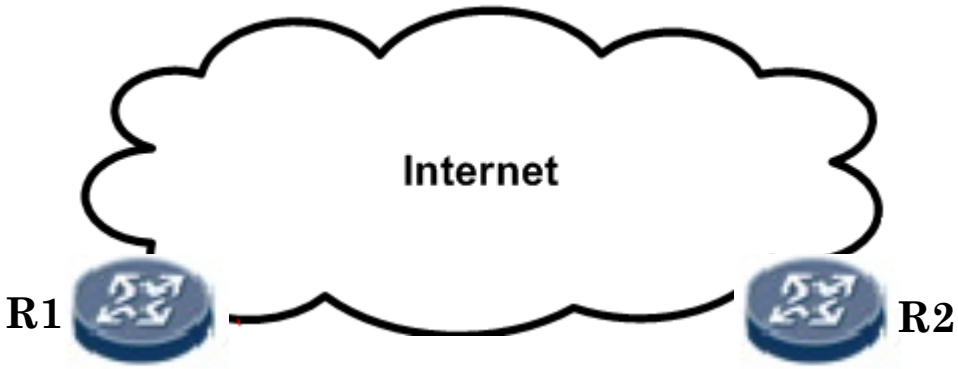
- Goal: Build forwarding table
  - Exchange messages with peers to share information
- Communication model
  - Unicast, multicast
- Communication transport
  - IP, UDP, TCP
- Prerequisite function
  - Identify peer routers (discover, configure)
- Security functions
  - Neighbor validity (authentication and authorization)
  - Message integrity

Routing Protocol Configuration

- Previous slide showed a variety of options
- Some routing protocols can be configured with variants
  - OSPF: IPsec or Authentication Trailer (AT)
    - AT can be MD5 or SHA1

- Neighbor relationships
  - IGPs (e.g., OSPF, PIM-SM) tend to "discover" neighbors
  - But ***should*** be told which ones are legitimate
  - EGPs (e.g., BGP) ***need*** to be told who their neighbors are

High Level View



- Routers

- Routing protocols


- Security mechanisms


Network Operator **Network Operator**

- Security management

?

- Configuration/ Distribution

Security Mechanism

- Message Integrity
  - Security protocol calculates authentication data using
    - Input = Routing protocol message + some credential
  - Today, the most-used credential is a Pre-shared key
- Security Association (SA) = security protocol + credential
- ***In practice, a router is both authenticated and authorized if it possesses the parameters of an SA***

Existing Security Mechanisms

- Two types
  - ***In-band*** and ***Out-of-band***
- ***In-band*** (part of the routing protocol exchanges)
  - Calculate the authentication data and attach it as a trailer to the routing protocol message
  - Keyed-MD5, HMACs
- ***Out-of-Band*** (part of the routing transport functionality)
  - TCP-MD5, TCP-AO
    - Calculate the authentication data and attach it to the TCP segment
  - IPsec
    - Calculate the authentication data and attach it to the IP header

Security Management

- Manual method for management of SA
  - If it is done at all,
  - it is (almost) never re-done.
- SA Management is:
  - Configuration/addition/deletion of an SA
- Current practice: device-by-device basis
  - Manual access: visit the router or access via remote CLI

Existing KMP standards

IETF Standard

- Unicast KMPs
  - IKEv1
  - IKEv2
- GKMP
  - GDOI
  - GSAKMP
- Work in progress
  - G-IKEv2
    - An updated version of GDOI

Work in progress

KMPs for Routing Protocol (KARP work)

- Unicast KMP
  - RKMP - based on IKEv2
- Group KMPs
  - G-IKEv2-MRKM
  - MaRK
  - Both based on G-IKEv2
- No solution has been standardized yet

- ***Parameters for KMPs are also configured manually***

Cryptographic Key Table (CKT)

- KARP working group standardized CKT (RFC7210)
- Stores master keys, key derivation functions and cryptographic protocols for the routing protocols

Common Security Parameters

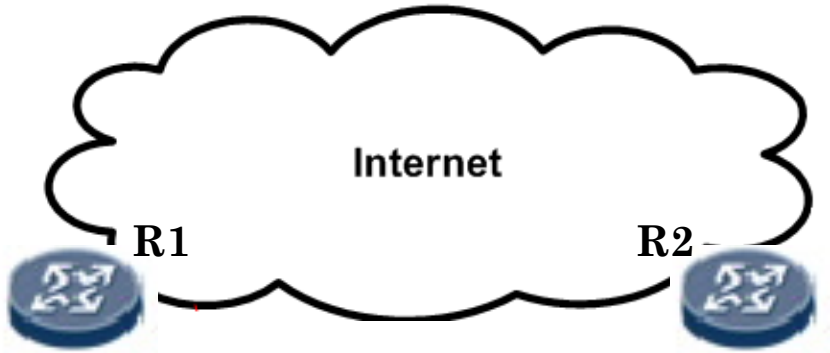
KMP requirements

- Peer Authentication -
  - **Peer identity**
  - **Peer credentials**
- SA Negotiation -
  - **List of security protocols**
  - **List of cryptographic algorithms**
- Deriving traffic keys for secure communications -
  - **Master key**
  - **Key derivation functions (KDF)**

Routing Protocol Security Requirements

- **Authentication**
- **Security protocol**
- **Keys**
  - **KDF**
  - **A master key**
- **Lifetime of key**

RECAP…



Security Management Framework

RP-1 ⟷ Message Exchange ⟷ RP-1

- **Layer 1**
  (Routing protocols)


- **Layer 2**
  (Security mechanisms)

KMP  KMP

negotiate/establish

- **Layer 3**
  (Security Management)

Common Security Parameters ?

Management Scheme ?

- **Layer 4**
  (Configuration/ Distribution)

Network Operator

Deficiencies at layers 3 and 4

Problem Statement

- To enhance the security of routing protocols

  1. A set of KMPs is required (**Layer 3**) (work in progress by others)

  2. A method for managing security parameters for routing protocols is required (**Layer 3**)
     a. ***Common security parameters***
  3. A management scheme for configuration and distribution of security parameters is required (**Layer 4**)
     a. ***Management modules for security parameters***

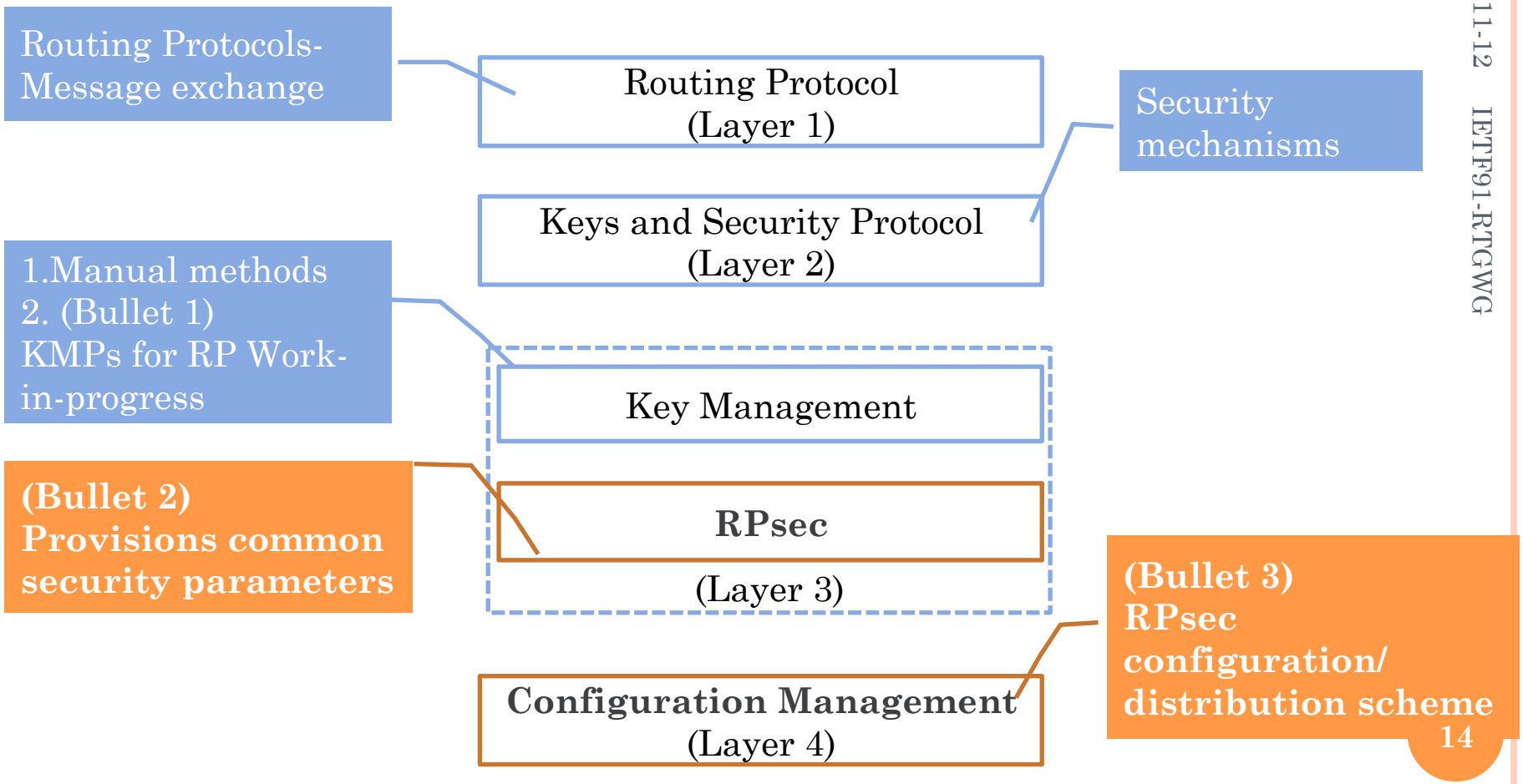
- Goals 2 and 3 have no work under way, to our knowledge

- There is a need to improve the ***security management framework*** for the routing protocols

Proposal

- **Routing Protocol Security (RPsec)**
- Improve the present security management framework of the routing protocols
- Mitigate the identified deficiencies
  - Layer 3: Security Parameter Management
  - Layer 4: Configuration and Distribution Management
- RPsec will enable a shift from present manual methods to fully automated methods
- RPsec will make a secure routing infrastructure easier to achieve

How RPsec Fits into the Present Security Management Framework



Acknowledgment

- Initial proposal was in KARP at IETF-87 (Berlin July 2013)
  - draft-atwood-karp-aapm-rp
    - Suggested ***authentication, authorization and policy management*** for routing protocols
    - Sam Hartman and Dacheng Zhang suggested using a Routing Authentication Policy Database (RAPD) with the CKT
- Updated for IETF-88 (Vancouver Nov 2013) but not presented
  - draft-zhang-karp-rapd
    - A more detailed specification of role of RAPD—Authentication and Authorization only.
    - Separated from the policy management aspects
- RPsec is the continuation of the above efforts

Design Objectives

- Independent of any specific security protocol
- Allows administrators to easily specify multiple security options for a routing protocol
- Accessible to multiple routing protocols implementations
- Accessible to multiple KMPs
- Provides support for both unicast and multicast routing protocol communication models

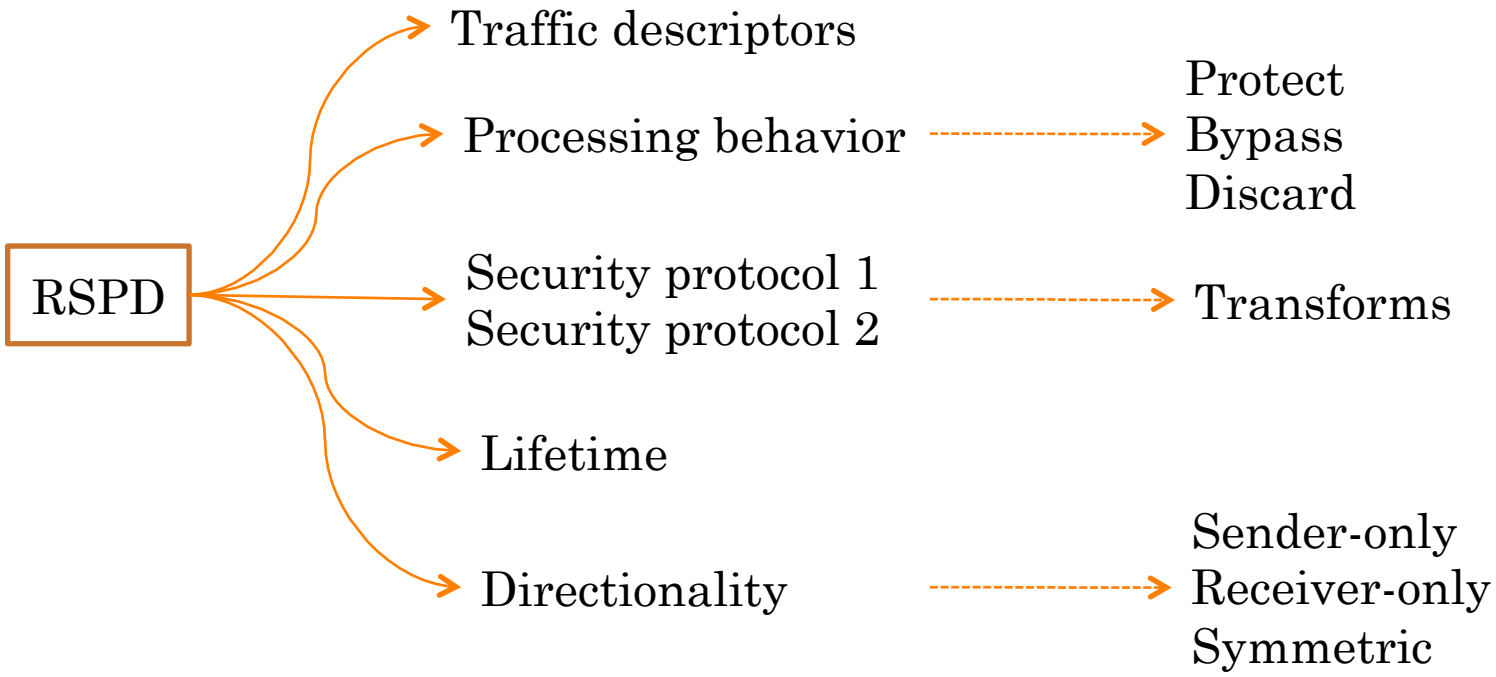
Overview

- Three component databases---
  - Provide peer authorization information
  - Security protocol choices
  - Key related parameters

- Role
  - A support module for key/SA management (at Layer 3)
  - KM methods will use RPsec for authentication and key/SA negotiation.
  - Routing protocol may consult RPsec directly for security parameters.

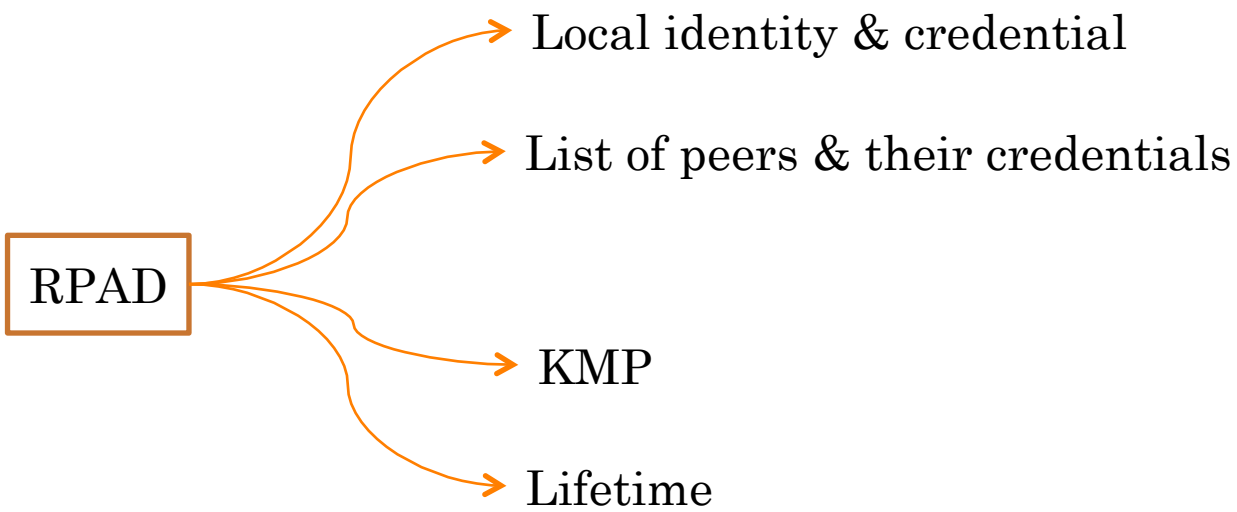
RSPD

- Objective
  - Specify the processing behavior for the identified routing protocol traffic.
  - Provide administrators the flexibility to specify multiple security options with associated lifetime information
  - A KMP uses the RSPD for SA negotiation



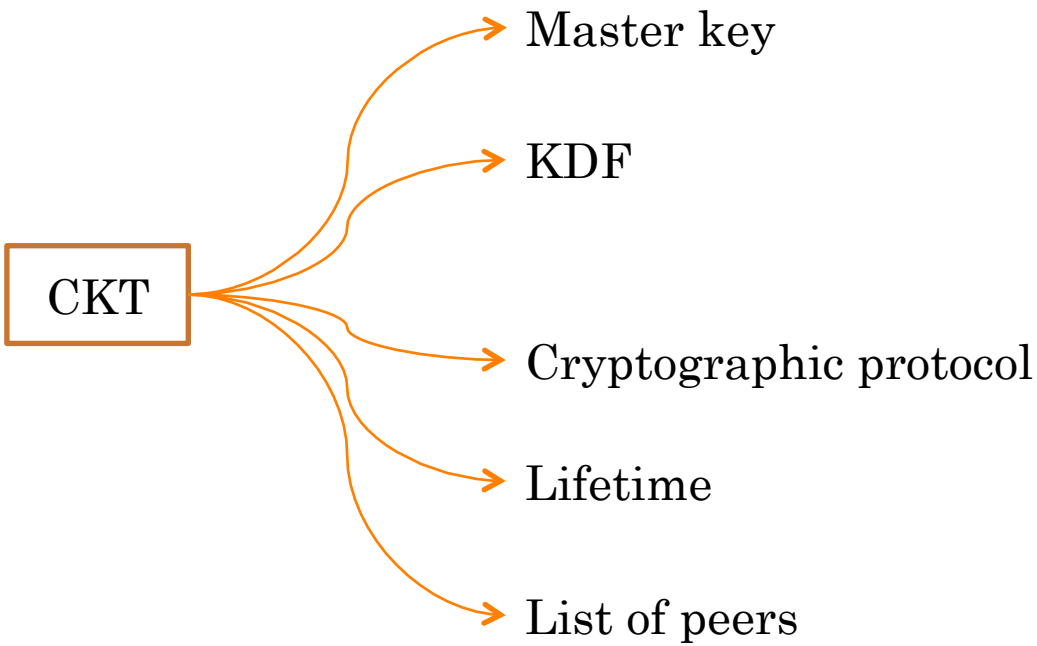
RPAD

- Objective
  - Stores authentication data and a KMP specification for the identified routing peers.
  - A KMP will use authentication data to assert a local/peer device's identity



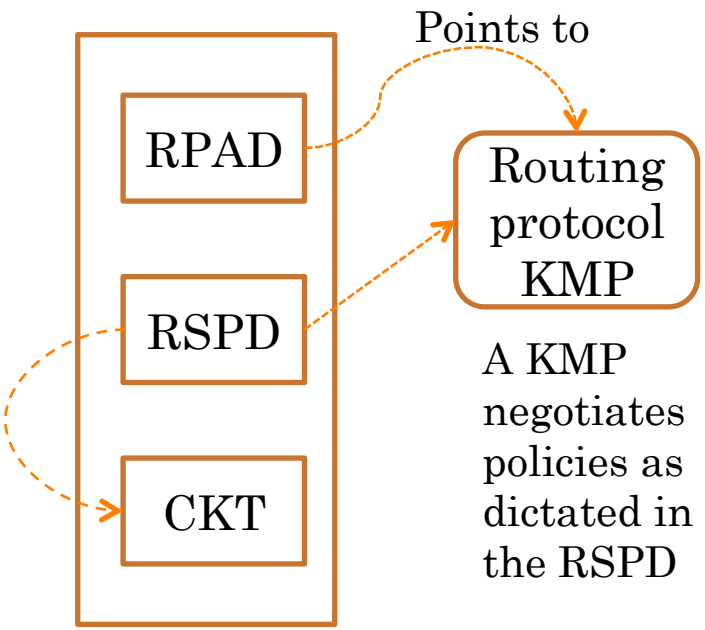
CKT

- Provisions key material and associated cryptographic algorithms
- The RSPD and CKT are used together to ensure that the key is provided to the security protocol that is used for securing the routing protocol.



Relation Between RPsec Databases

Each entry in RSPD points to a corresponding entry in CKT,



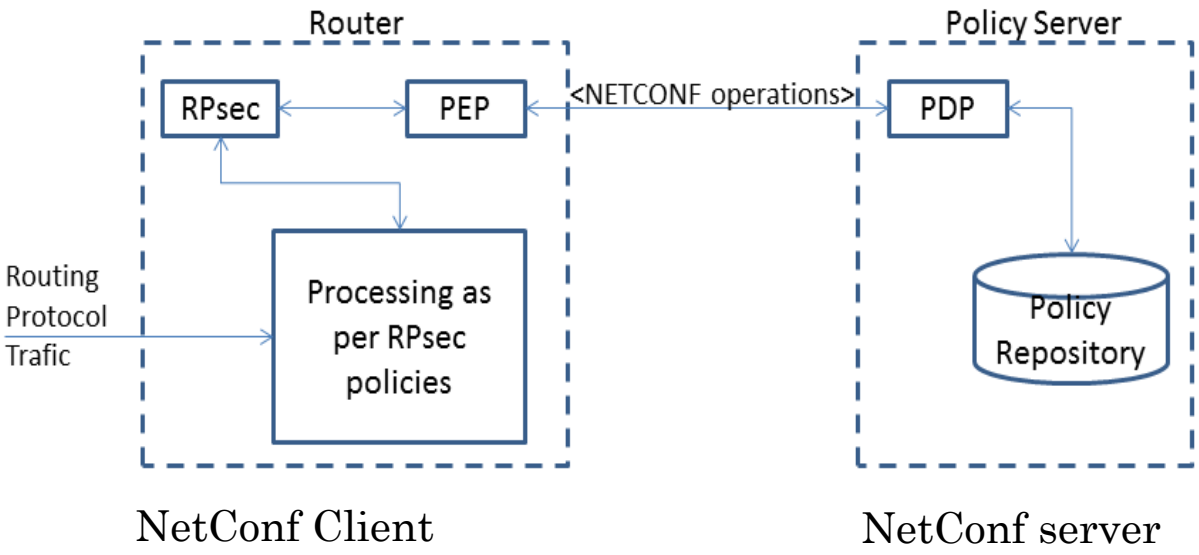
A KMP negotiates policies as dictated in the RSPD

RPsec Yang Modules

- We have specified the options for the security parameters in four Yang modules for the RPsec
  - rpsec-common-types.yang
  - rspd.yang
  - rpad.yang
  - ckt.yang

- The RPsec Yang modules provide:
  - parameters for both unicast and multicast communication
  - logically structured entries in RSPD, RPAD and CKT

RPSEC CONFIGURATION/DISTRIBUTION ARCHITECTURE



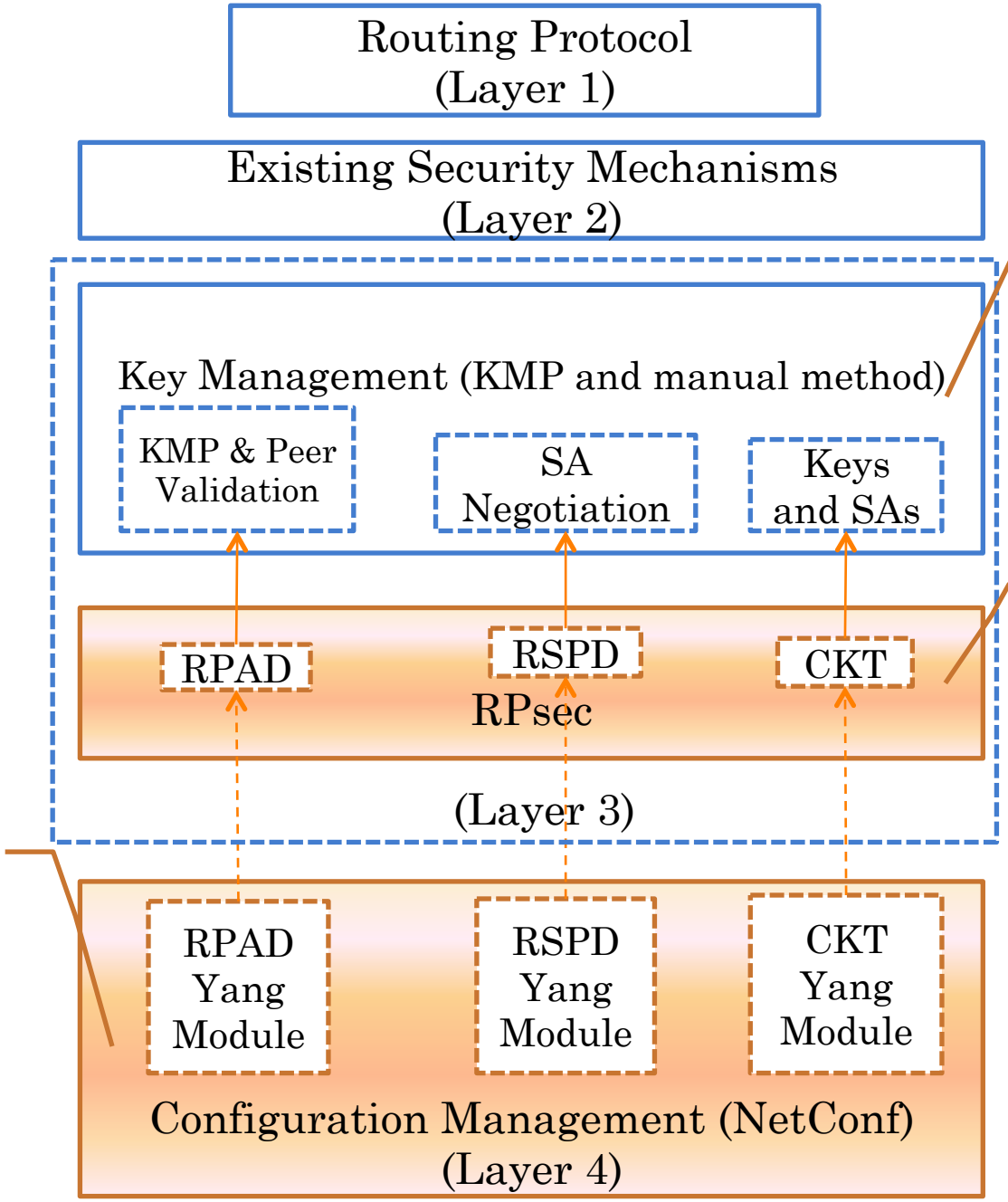
Send request for RPsec entries

Reply with or push RPsec entries

A Framework for Policy Admission Control

This architecture can also be scaled to a distributed architecture

RECAPITULATION



KMP negotiates SA and provides fresh keys to security protocol at layer 2

RPsec component databases

YANG modules for representation and configuration of RPsec databases

Summary of RPSec

- Provisions authentication information for the routing protocol peers.
- Provides support for KMPs for dynamic negotiation, establishment and rekey/rollover of SAs for the routing protocols when available.
- Administrators can specify multiple security mechanisms in the RSPD for the routing protocol.
- Overcomes the manual security configuration issues faced by the operators
  - Automated regular key changes for the routing protocols.
- Finally, provides four Yang modules that can be
  - easily modified and configured
  - distributed over the network.

Questions?

Thank you!